CLAIMS

What is claimed is:

1. A method for decoding a keystream, comprising:

receiving a set of cipher bits;

generating a set of test bits;

generating a set of attempted keystream bits from differences between the test bits and the cipher bits;

generating, from a current seed, a set of current keystream bits from a parallel feedback shift register;

comparing the attempted keystream bits to the current keystream bits;

feeding back the current keystream bits as a new current seed in response to attempted keystream bits that equal the current keystream bits; and

feeding back the attempted keystream bits as a new current seed in response to attempted keystream bits that do not equal the current keystream bits.

2. The method of claim 1, wherein the step of generating a set of current keystream bits includes generating the bits from a first set of function generators of a field programmable gate array (FPGA).

3. The method of claim 2, wherein the step of generating the attempted keystream bits and the step of comparing are performed on a second set of function generators of an FPGA.

4. The method of claim 3, wherein the step of generating a set of attempted keystream bits from differences between the test bits and the cipher bits includes applying an exclusive-or function to each bit of the test bits and a corresponding bit of the cipher bits.

5. The method of claim 4, wherein the step of comparing the attempted keystream bits to the current keystream bits

includes applying an exclusive-or function to each bit of the attempted keystream bits and a corresponding bit of the current keystream bits.

6. The method of claim 1, further comprising signaling that the keystream is decoded in response to the attempted keystream bits being equal to the current keystream bits.

7. A method for decoding a keystream, comprising:

(a) receiving a set of cipher bits;

(b) generating a current set of test bits;

(c) generating a set of attempted keystream bits from differences between the current set of test bits and the cipher bits;

(d) generating, from a current seed, a set of current keystream bits from a parallel feedback shift register;

(e) comparing the attempted keystream bits to the current keystream bits;

(f) feeding back the current keystream bits as a new current seed in response to attempted keystream bits that equal the current keystream bits;

(g) feeding back the attempted keystream bits as a new current seed in response to attempted keystream bits that do not equal the current keystream bits;

(h) signaling that the keystream is decoded in response to the attempted keystream bits being equal to the current keystream bits;

(i) in response to the attempted keystream bits being not equal to the current keystream bits,

(j) generating a new current set of test bits, the new current set of test bits being one of a plurality of sets of test bits, wherein no two sets of test bits have identical bit values;

(k) repeating steps (a) - (j) until each of the plurality of sets of test bits has been generated; and

(l) in response to the attempted keystream bits being not equal to the current keystream bits and having generated each of the plurality of sets of test bits,

(m) receiving a new plurality of cipher bits; and

(n) repeating steps (a) - (m) until the attempted keystream bits are equal to the current keystream bits.

8. The method of claim 7, wherein the step of generating a set of current keystream bits includes generating the bits from a first set of function generators of a field programmable gate array (FPGA).

9. The method of claim 8, wherein the step of generating the attempted keystream bits and the step of comparing are performed on a second set of function generators of an FPGA.

10. The method of claim 9, wherein the step of generating a set of attempted keystream bits from differences between the test bits and the cipher bits includes applying an exclusive-or function to each bit of the test bits and a corresponding bit of the cipher bits.

11. The method of claim 10, wherein the step of comparing the attempted keystream bits to the current keystream bits includes applying an exclusive-or function to each bit of the attempted keystream bits and a corresponding bit of the current keystream bits.

12. A parallel keystream decoder, comprising:

a first circuit configured to generate a set of test bits;

a second circuit coupled to the first circuit, the second circuit configured to generate a set of attempted keystream bits from differences between the test bits and an input set of cipher bits;

a parallel feedback shift register (PFSR) configured to generate, from a current seed, a set of current keystream bits;

a third circuit coupled to the PFSR and to the second circuit, the third circuit configured to compare the attempted keystream bits to the current keystream bits; and

a fourth circuit coupled to the third circuit, the fourth circuit configured to feed back the current keystream bits as a new current seed in response to attempted keystream bits that equal the current keystream bits, and feed back the attempted keystream bits as a new current seed in response to attempted keystream bits that do not equal the current keystream bits.

13. The decoder of claim 12, wherein the parallel feedback shift register is configured in a first set of function generators of a field programmable gate array (FPGA).

14. The decoder of claim 13, wherein the second third circuits are configured in a second set of function generators of an FPGA.

15. The decoder of claim 14, wherein the second set of function generators are configured to implement exclusive-or functions between the test bits and the cipher bits.

16. The decoder of claim 15, wherein the second set of function generators are configured to implement exclusive-or functions between the attempted keystream bits and the current keystream bits.

17. The decoder of claim 12, further comprising a fifth circuit coupled to third circuit, the fifth circuit configured to signal that the keystream is decoded in response to the attempted keystream bits being equal to the current keystream bits.

18. An *n*-bit parallel feedback shift register, wherein *n* is greater than 3, comprising:

n single-bit registers in a field programmable gate array (FPGA); and

n function generators in the FPGA, each function generator having an output port coupled to a respective one of the registers and a plurality of input ports coupled to output ports of at least two of the registers, wherein each function generator is configured to apply an exclusive-or function to signals at the input ports, and each register is updated with a new state in response to output from the coupled function generator.